ЛЕКЦИЯ 3

НОРМАЛЬНОЕ ЗАМЫКАНИЕ ГРУПП

ГОМОМОРФИЗМЫ ГРУПП

ФАКТОР-ГРУППЫ

ПЕРВАЯ ТЕОРЕМА О ГОМОМОРФИЗМЕ

НОРМАЛЬНОЕ ЗАМЫКАНИЕ ГРУПП

Лемма 1. *Если* $\{H_i,\ i \in I\}$ *— совокупность нормальных подгрупп группы* G, $H_i \lhd G$, *то* $H = \bigcap\limits_{i \in I} H_i$ *— нормальная подгруппа группы* G.

Доказательство. Действительно, мы знаем, что H — подгруппа. Если $h \in H$ и $g \in G$, то $h \in H_i$ для всех $i \in I$, и так как $H_i \lhd G$, то $g^{-1}hg \in H_i$ для всех $i \in I$. Поэтому $g^{-1}hg \in \bigcap\limits_{i \in I} H_i = H$. Итак, $H \lhd G$. □

Пусть S — непустое подмножество группы G. Рассмотрим совокупность всех нормальных подгрупп $H_i \lhd G$, $i \in I$, таких, что $S \subseteq H_i$ (эта совокупность непуста, поскольку она содержит саму группу G). Тогда

$$S \subseteq N(S) = \bigcap_{i \in I} H_i \lhd G.$$

Покажем в следующей теореме, что: $N(S)$ — *наименьшая нормальная подгруппа, содержащая* S; если

$$S^G = \{g^{-1}sg \mid s \in S,\ g \in G\},$$

то оказывается, что подгруппа $\langle S^G \rangle$, порожденная подмножеством S^G, является наименьшей нормальной подгруппой, содержащей S, и потому она совпадает с $N(S)$.

Теорема 1 (о нормальном замыкании подмножества группы)**.** *Пусть* S *— непустое подмножество группы* G*. Тогда*:

1) *пересечение*
$$N(S) = \bigcap_{S\subseteq N_i \lhd G} N_i$$
всех нормальных подгрупп $N_i \lhd G$ *таких, что* $S \subseteq N_i$*, является наименьшей нормальной подгруппой группы* G*, содержащей подмножество* S;

2) $N(S) = \langle S^G \rangle = \left\{ \prod\limits_{k=1}^{t} g_k^{-1} s_k^{\pm 1} g_k \;\middle|\; t \in \mathbb{N},\; s_k \in S,\; g_k \in G \right\}$ (*элементы нормального замыкания подмножества* S *в группе* G *— это в точности конечные произведения элементов вида* $g^{-1}s^{\pm 1}g$*,* $s \in S$*,* $g \in G$).

Доказательство. 1) Так как пересечение нормальных подгрупп — нормальная подгруппа, то $N = \bigcap N_i \lhd G$. Ясно, что $S \subseteq N = \bigcap N_i$, поскольку $S \subseteq N_i$ для всех $\{N_i \lhd G \mid S \subseteq N_i,\; i \in I\}$ (это множество содержит $N_i = G$, и поэтому не является пустым). Таким образом, нормальная подгруппа N, $S \subseteq N$, сама принадлежит этому множеству, т. е. $N = N_i$ для некоторого $i \in I$, и следовательно, $N = \bigcap\limits_{S\subseteq N_i \lhd G} N_i$.

2) В силу 1) из $S \subseteq N \lhd G$ следует, что
$$\langle S^G \rangle = \left\{ \prod_{k=1}^{t} g_k^{-1} s_k^{\pm 1} g_k \;\middle|\; t \in \mathbb{N},\; s_k \in S,\; g_k \in G \right\} \subseteq N.$$
Но ясно, что $\langle S^G \rangle$ — нормальная подгруппа в G, содержащая S. Таким образом, $N \subseteq \langle S^G \rangle$. Итак, $\langle S^G \rangle = N$, и мы имеем общий вид произвольного элемента нормального замыкания $N(S)$. $\square$

ГОМОМОРФИЗМЫ ГРУПП

Пусть G и G' — группы. Напомним, что отображение $f\colon G \to G'$, для которого $f(ab) = f(a)f(b)$ для всех элементов $a, b \in G$, называется *гомоморфизмом*. Биективные гомоморфизмы называются *изоморфизмами*.

Пример 1. Пусть $G = \mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$ с операцией умножения, $G' = (\mathbb{R}, +)$ с операцией сложения. Так как для отображения $\ln\colon \mathbb{R}^+ \to \mathbb{R}$ имеем $\ln(ab) = \ln(a) + \ln(b)$ для всех $a, b \in \mathbb{R}^+$, то $\ln$ — гомоморфизм групп. Так как это — биекция, то $\ln$ — изоморфизм.

Пример 2. Если $G = \mathbf{S}_n$ — группа подстановок и $G' = \{1, -1\}$ — группа с операцией умножения, то отображение $\varepsilon\colon \mathbf{S}_n \to \{1, -1\}$, для которого $\varepsilon(\sigma) = 1$, если $\sigma \in \mathbf{A}_n$, т. е. если σ — четная подстановка, и $\varepsilon(\sigma) = -1$ для $\sigma \in \mathbf{S}_n \setminus \mathbf{A}_n$, т. е. для нечетной подстановки σ, является гомоморфизмом групп, поскольку $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$ для всех $\sigma, \tau \in \mathbf{S}_n$.

Пример 3. Пусть $G = \mathrm{GL}_n(\mathbb{R})$, $G' = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ с операцией умножения. Так как $|AB| = |A|\,|B|$ для $A, B \in \mathrm{GL}_n(\mathbb{R})$, то отображение $A \mapsto |A|$ из $\mathrm{GL}_n(\mathbb{R})$ в $\mathbb{R}^*$, ставящее в соответствие матрице A ее определитель $|A|$, является гомоморфизмом групп.

Упражнение 1. Найдите все гомоморфизмы $f\colon G \to G'$, где $G = \langle a \rangle$, $O(a) = m$, $G' = \langle b \rangle$, $O(b) = n$ (в частности, для $m = 12$, $n = 15$).

Для гомоморфизмов $f\colon G \to G'$ определим:

$$\operatorname{Im} f = \{g' \in G' \mid g' = f(g) \text{ для } g \in G\}$$

(*образ* гомоморфизма f);

$$\ker f = \{g \in G \mid f(g) = e'\},$$

где e' — нейтральный элемент группы G' (*ядро* гомоморфизма f).

Теорема 2 (свойства гомоморфизма групп)**.** *Пусть G и G' — группы, e и e' соответственно — их нейтральные элементы, $f\colon G \to G'$ — гомоморфизм групп. Тогда*:

1) $f(e) = e'$;

2) $f(x^{-1}) = \big(f(x)\big)^{-1}$ *для всех* $x \in G$;

3) $H' = \operatorname{Im} f$ *— подгруппа группы G';*

4) *если $G = \langle a \rangle$ — циклическая группа, то* $\operatorname{Im} f = \langle f(a) \rangle$ *— также циклическая группа;*

5) *если $O(a) < \infty$ для $a \in G$, то $O\big(f(a)\big)$ является делителем числа $O(a)$ (если f — инъективный гомоморфизм, то $O\big(f(a)\big) = O(a)$);*

6) $f(g^{-1}hg) = \big(f(g)\big)^{-1} f(h) f(g)$;

7) $\ker f$ *— нормальная подгруппа группы* G;

8) *для $x, y \in G$ $f(x) = f(y)$ тогда и только тогда, когда* $xy^{-1} \in \ker f$;

9) *f — инъективное отображение тогда и только тогда, когда* $\ker f = \{e\}$.

Доказательство. 1) Так как $u = f(e) = f(e^2) = f(e)f(e) = u^2$, то $u = e'$, т. е. $f(e) = e'$.

2) Так как $f(x^{-1})f(x) = f(x^{-1}x) = f(e) = e'$ и $f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$, то $f(x^{-1}) = \big(f(x)\big)^{-1}$.

3) Если $h'_1 = f(g_1)$ и $h'_2 = f(g_2)$ — элементы из $\operatorname{Im} f$, где $g_1, g_2 \in G$, то

$$h'_1 h'_2 = f(g_1)f(g_2) = f(g_1 g_2) \in \operatorname{Im} f.$$

Если $h' = f(g) \in \operatorname{Im} f$, $g \in G$, то

$$(h')^{-1} = \big(f(g)\big)^{-1} = f(g^{-1}) \in \operatorname{Im} f.$$

Итак, $\operatorname{Im} f$ — подгруппа группы G'.

4) Если $G = \langle a \rangle$ и $h' \in \operatorname{Im} f$, $h' = f(g)$, $g \in G$, то $g = a^n$, $n \in \mathbb{Z}$, и поэтому

$$h' = f(g) = f(a^n) = \big(f(a)\big)^n.$$

Итак, $\operatorname{Im} f = \langle f(a) \rangle$ — циклическая группа с образующим $f(a)$.

5) Пусть $n = O(a)$. Тогда $a^n = e$, и поэтому

$$\big(f(a)\big)^n = f(a^n) = f(e) = e'.$$

Следовательно, число $O\big(f(a)\big)$ является делителем числа $n = O(a)$.

Если же f — инъективный гомоморфизм и $m = O\big(f(a)\big)$, то

$$e' = \big(f(a)\big)^m = f(a^m),$$

поэтому $a^m = e$, и следовательно, $n = O(a)$ является делителем числа m. Таким образом, $O(a) = n = m = O\big(f(a)\big)$.

6) следует из 2).

7) Если $h_1, h_2 \in H = \ker f$, то $f(h_1) = e'$, $f(h_2) = e'$. Поэтому $f(h_1 h_2) = f(h_1) f(h_2) = e' \cdot e' = e'$, т. е. $h_1 h_2 \in \ker f$.

Если $h \in \ker f$, то $f(h) = e'$, и поэтому $f(h^{-1}) = \big(f(h)\big)^{-1} = (e')^{-1} = e'$, т. е. $h^{-1} \in \ker f$. Таким образом, $\ker f$ — подгруппа группы G.

Если $h \in H = \ker f$, то $f(h) = e'$. Для любого элемента $g \in G$ имеем

$$f(g^{-1} h g) = f(g^{-1}) f(h) f(g) = f(g)^{-1} e' f(g) = e'.$$

Таким образом, $g^{-1}(\ker f) g \subseteq \ker f$ для всех элементов $g \in G$, т. е. $\ker f$ — нормальная подгруппа группы G.

8) $f(x) = f(y) \iff e' = f(x) f(y)^{-1} = f(x) f(y^{-1}) = f(x y^{-1}) \iff x y^{-1} \in \ker f$.

9) а) Если $\ker f = \{e\}$, то из $f(x) = f(y)$ следует, что $x y^{-1} = e$, т. е. что $x = y$, другими словами, f — инъективное отображение.

б) Если f — инъективное отображение, то, так как $f(e) = e'$, из $f(x) = e'$ следует, что $x = e$, т. е. $\ker f = \{e\}$. $\square$

Упражнение 2. В рассмотренных выше примерах гомоморфизмов групп найти образ и ядро гомоморфизма.

Упражнение 3. Докажите, что не существует сюръективного гомоморфизма $(\mathbb{Q}, +) \to (\mathbb{Z}, +)$.

ФАКТОР-ГРУППЫ, КАНОНИЧЕСКИЙ ГОМОМОРФИЗМ

Пусть G — группа, H — ее нормальная подгруппа, $G/H = \{xH = Hx \mid x \in G\}$ — множество смежных классов по подгруппе H. Определим на множестве G/H операцию умножения, полагая $xH \cdot yH = xyH$.

Проверим *корректность* этого определения (т. е. что умножение смежных классов не зависит от выбора их представителей).

Действительно, пусть $xH = x'H$, $yH = y'H$. Тогда $x' = xh_1$, $y' = yh_2$, где $h_1, h_2 \in H$. Следовательно, $x'y' = xh_1yh_2 = xyh_1'h_2$, где $h_1y = yh_1'$ (поскольку $Hy = yH$) для $h_1' \in H$. Так как $h_1'h_2 \in H$, то $x'y' = xyh_1'h_2 \in xyH$, и поэтому $x'y'H = xyH$.

Для любых $x, y, z \in G$ имеем

$$(xHyH)zH = (xy)zH = x(yz)H = xH(yHzH),$$

т. е. операция умножения смежных классов ассоциативна.

Ясно, что для $H = eH$ имеем

$$eHxH = exH = xH = xeH = xHeH$$

для всех $xH \in G/H$, т. е. $H = eH$ — нейтральный элемент.

Для всякого $xH \in G/H$ из

$$(xH)(x^{-1}H) = xx^{-1}H = eH = H,$$
$$(x^{-1}H)(xH) = x^{-1}xH = eH = H$$

получаем, что $(xH)^{-1} = x^{-1}H$, т. е. у каждого смежного класса xH имеется обратный элемент $(xH)^{-1} = x^{-1}H$.

Таким образом, мы доказали первое утверждение следующей теоремы.

Теорема 3. *Если $H \lhd G$, то*:

1) *множество смежных классов $G/H = \{xH = Hx \mid x \in G\}$ группы G по ее нормальной подгруппе $H \lhd G$ с операцией $xH \cdot yH = xyH$ является группой* (*называемой* фактор-группой группы G по нормальной подгруппе H);

2) *отображение $\pi = \pi_H \colon G \to G/H$, для которого $\pi(x) = xH$, $x \in G$, является сюръективным гомоморфизмом* (*называемым* каноническим гомоморфизмом);

3) $\ker \pi_H = H$;

4) *если $|G| < \infty$, то $|G/H| = \frac{|G|}{|H|} = (G : H)$.*

Доказательство. Осталось проверить 2), 3) и 4). Действительно, для $a, b \in G$ имеем

$$\pi(ab) = abH = aH \cdot bH = \pi(a)\pi(b),$$

т. е. $\pi = \pi_H$ — гомоморфизм.

Если $g \in G$, то $gH = \pi(g)$, т. е. π — сюръекция.

Если $a \in G$, то $a \in \ker \pi_H$ тогда и только тогда, когда $\pi(a) = aH = H$. Но это равносильно тому, что $a \in H$. Итак, $\ker \pi_H = H$.

4) следует из теоремы Лагранжа. $\square$

Следствие 1. *Нормальные подгруппы H группы G и только они являются ядрами гомоморфизмов $f \colon G \to G'$ из группы G во все группы G'.*

ПРИМЕРЫ ФАКТОР-ГРУПП

1) Пусть $H = \{e\} \lhd G$. Тогда $x\{e\} = x$ для всех $x \in G$, т. е. все смежные классы по единичной подгруппе — это в точности одноэлементные подмножества, т. е. элементы группы G, при этом

$$x\{e\} \cdot y\{e\} = xy\{e\} = xy.$$

Таким образом, биекция $x\{e\} \mapsto x$, $G/\{e\} \to G$ является изоморфизмом групп.

2) Пусть $H = G \lhd G$. Тогда имеем один смежный класс $\bar{e} = eG = G$. Итак, $G/G = \{\bar{e}\}$, $|G/G| = 1$.

3) Группа $\mathbb{Z}_n$ вычетов по модулю n как фактор-группа группы $(\mathbb{Z}, +)$ по подгруппе $n\mathbb{Z}$. Пусть $G = \mathbb{Z}$ — группа целых чисел с операцией сложения, n — натуральное число и $H = n\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\}$ — подгруппа целых чисел, делящихся на n. Для $k \in \mathbb{Z}$ рассмотрим смежный класс

$$C_k = k + n\mathbb{Z} = \{k + nq \mid q \in \mathbb{Z}\}.$$

Ясно, что $C_k = C_l$ для $l \in \mathbb{Z}$ тогда и только тогда, когда $k - l = nq$. Так как $k = nq + r$, где $q \in \mathbb{Z}$, $0 \leqslant r < n$, то $C_k = C_r$. Таким образом, множество всех различных смежных классов $\mathbb{Z}_n = G/H = \mathbb{Z}/n\mathbb{Z} = \{C_0, C_1, \ldots, C_{n-1}\}$ находится в биективном соответствии с остатками $\{0, 1, 2, \ldots, n-1\}$ при делении на число n. Если $k, l \in \mathbb{Z}$ и $k + l = nq + r$, то

$$C_k + C_l = (k + n\mathbb{Z}) + (l + n\mathbb{Z}) = (k + l) + n\mathbb{Z} = r + n\mathbb{Z} = C_r.$$

Таким образом, операция сложения фактор-группы $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ в точности соответствует операции сложения остатков при делении на n по модулю числа n (т. е. сначала надо сложить остатки как целые числа, а затем от суммы взять остаток при ее делении на n). Таким образом, $\mathbb{Z}_n$ — группа.

4) В фактор-группе $\mathbb{Q}/\mathbb{Z}$ любой элемент имеет конечный порядок; для любого натурального числа n существует единственная подгруппа группы $\mathbb{Q}/\mathbb{Z}$ порядка n.

5) Фактор-группа $\mathbb{R}/\mathbb{Z}$ имеет естественную интерпретацию как группа $T = \{z \in \mathbb{C} \mid |z| = 1\}$ единичной окружности (или поворотов плоскости вокруг начала координат против часовой стрелки на угол φ, что равносильно умножению на комплексное число $\cos\varphi + i\sin\varphi$), а именно биекция

$$f\colon \mathbb{R}/\mathbb{Z} \to T, \quad f(r+\mathbb{Z}) = \cos 2\pi r + i\sin 2\pi r,$$

осуществляет изоморфизм групп $\mathbb{R}/\mathbb{Z}$ и T.

ПЕРВАЯ ТЕОРЕМА О ГОМОМОРФИЗМЕ

Теорема 4 (о гомоморфизме для групп)**.** *Пусть* $f\colon G \to G'$ *— сюръективный гомоморфизм (т. е. гомоморфизм из группы* G на *группу* G'*). Тогда существует изоморфизм*

$$\psi\colon G/\ker f \to G'$$

такой, что $f = \psi\pi$*, где* $\pi\colon G \to G/\ker f$ *— канонический гомоморфизм из группы* G *на фактор-группу* $G/\ker f$ *по нормальной подгруппе* $\ker f$ *(ядро гомоморфизма* f*).*

Доказательство. Для смежного класса $x\ker f$, $x \in G$, положим $\psi(x\ker f) = f(x)$.

Корректность отображения $\psi\colon G/\ker f \to G'$. Если для $y \in G$ имеем $x\ker f = y\ker f$, то $x^{-1}y \in \ker f$, поэтому $e' = f(x^{-1}y) = f(x)^{-1}f(y)$, следовательно, $f(x) = f(y)$.

Покажем, что ψ — *биекция.*

а) Если для $x, y \in G$ имеем $f(x) = \psi(x\ker f) = \psi(y\ker f) = f(y)$, то $f(x^{-1}y) = f(x)^{-1}f(y) = e'$, т. е. $x^{-1}y \in \ker f$. Поэтому $x\ker f = y\ker f$, т. е. ψ — инъекция.

б) Если $g' \in G'$, то $g' = f(x)$ для некоторого $x \in G$ (поскольку f — сюръекция). Тогда $g' = f(x) = \psi(x\ker f)$, т. е. ψ — сюръекция.

Проверим, что ψ — *гомоморфизм* групп. Действительно, для $x, y \in G$ имеем

$$\psi(x\ker f \cdot y\ker f) = \psi(xy\ker f) = f(xy) = \\ = f(x)f(y) = \psi(x\ker f)\psi(y\ker f).$$

Итак, мы показали, что $\psi\colon G/\ker f \to G'$ — *изоморфизм*.

Проверим, что $f = \psi\pi$. Действительно, для $x \in G$ имеем

$$(\psi\pi)(x) = \psi\big(\pi(x)\big) = \psi(x\ker f) = f(x). \qquad \square$$

Теорема о гомоморфизме является эффективным средством для вычисления фактор-групп.

Пример 4. Пусть $G = (\mathbb{C}^*, \cdot)$, $H = (\mathbb{R}^*, \cdot) \subset G$.

Рассмотрим сюръективный гомоморфизм

$$f\colon G = \mathbb{C}^* \to T = \{z \in \mathbb{C} \mid |z| = 1\},$$

для которого $f(z) = \frac{z^2}{|z|^2}$ для $z \in \mathbb{C}^*$. Тогда $\ker f = H = \{\mathbb{R}^*, \cdot\}$. В силу теоремы о гомоморфизме

$$T \cong G/\ker f = \mathbb{C}^*/\mathbb{R}^*. \qquad \square$$